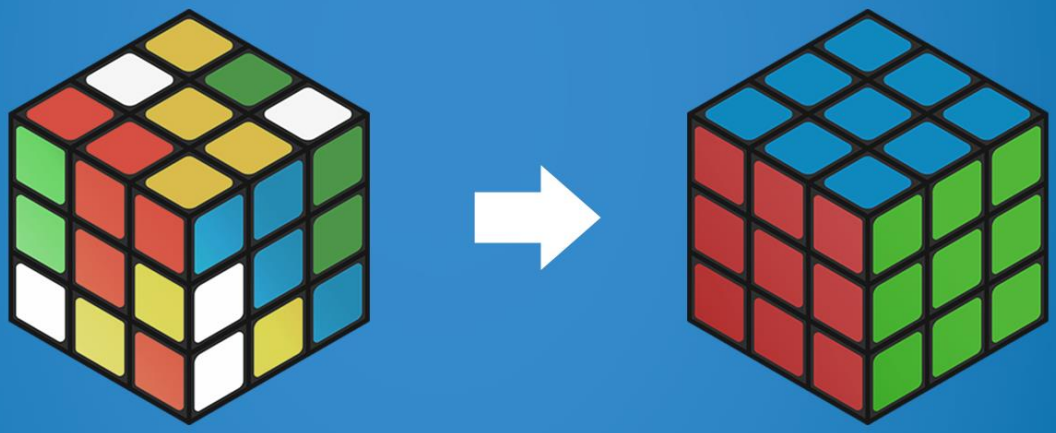
A FRAMEWORK TO

SIMPLIFY

SMB I.T.



hersTek.com

The cyber environment is growing increasingly complex. With new cyber risks, more remote workers, and IT evolving, it can be a lot for a small business owner to manage.

This eBook shares a framework for essential tech that every business needs.

CYBER NEEDS CHANGE
AND GROW MORE CHALLENGING

The small business is famous for needing everyone to pitch in in several different areas. You'll see the owner or, if there is one, office manager taking charge of ordering business technology. Individuals download their own software choices without strategy behind the purchases. If someone needs tech support, the most computer savvy at work figures it out. Everyone assumes the manufacturers of the various technologies are taking care of security.

The global migration to remote work also adds challenges. Those employees working from home are often doing so from their own devices, and they may be using home Wi-Fi networks. Now, your business network stretches well beyond the bounds of your on-premises firewall. Plus, employees continue to download third-party apps you don't know about and that could be compromising their technology. When they connect to your network, your business gets compromised, too.

At the same time, cybercrime threats are increasing. The number of potential entry points to identify and protect is constantly growing. Bad actors remain highly motivated to attack small business targets. Plus, they are finding ways to take advantage of the new vulnerabilities remote workers represent.

There is just so much IT, it's difficult to keep up with it all. We find it's useful to think about all these IT issues in terms of a four-part framework:

- tech stack;
- security and compliance;
- IT Management ;
- IT Operations.

Looking at technology this way, your small business can better identify IT gaps.

Next, we'll explain the differences between each area in small business tech strategy.

WHY IS I.T. SO COMPLEX?

To frustrate SMBs. No, not really. But it can feel that way, right?

Business technology is complicated because:

- virtually every business has had to embrace digital transformation;
- every business needs 24/7 uptime and data protection;
- Although cloud computing improves collaboration and agility, it extends the business attack surface;
- most everyone has a computer in their pocket in the form of a smartphone, and they want to use it at work.
- people download unapproved apps to their devices to be more productive, but add risk;
- customer and industry expectations for data security controls are rising;
- cybercriminals continue to target businesses with myriad types of attack.

TECH STACK

You don’t actually stack all your business technology, yet every small business today has a tech stack.

Does anyone at your small business actually understand the full range of technology? We're not just talking about troubleshooting the printer or personal computers. The tech stack includes your routers, switches, firewall, storage, database, and servers. You might have workstations in the cloud and on-premises. Those are part of the tech stack, too.

The tech stack is also known as IT infrastructure. It consists of everything your business uses to function. That’s client-facing technology and back-end stuff (operating systems, servers, data storage, and more). You may also have some API services that help you connect different tech stack segments.

Your people need to be confident in the tech stack to get their jobs done. Those in charge of the tech stack focus on reliability, flexibility, and scalability. Budget considerations rank high, too.

SECURITY
AND COMPLIANCE

Every business is at risk of cyberattack. Depending on your industry, you may also face regulatory processes. You might need to comply with security control regulations in healthcare or payment processing or protect personally identifiable information (PII).

No matter the size of your business, you need to:

- **identify** – understand cybersecurity risk to systems, people, assets, data, and capabilities;
- **protect** – safeguard your infrastructure and limit or contain the impact of a potential cybersecurity event;
- **detect** – identify the occurrence of a cybersecurity event in a timely fashion;
- **respond** – take action to contain the impact of a potential cybersecurity incident;
- **recover** – plan for resilience and to restore any capabilities or services impaired due to a cybersecurity incident.

Your small business needs to keep its technology current and patch against vulnerabilities. But successful security and compliance also requires IT controls. These include multi-factor authentication, identity and access management, encryption, and malware protection.

IT MANAGEMENT

IT management and IT operations may sound like the same thing, but there are distinctions.

IT management uses a vast array of tools to monitor and manage all business IT assets. They know what hardware and software is deployed and how it's used, and take charge of any upgrades.

The IT management area handles end-to-end delivery of IT services. They manage all infrastructure and system changes working to ensure minimal disruption.

This is also the area that covers the help desk. Probably with more confidence than Jorge, who you actually hired as an accountant. Access requests or password resets? That’s IT management. Plus, this area handles bigger problems and also does analysis to prevent a recurrence.

IT OPERATIONS

IT operations makes sure business technology is up and running so that users can be at their most productive. They establish the processes and procedures to monitor performance and manage availability. They are responsible for improving:

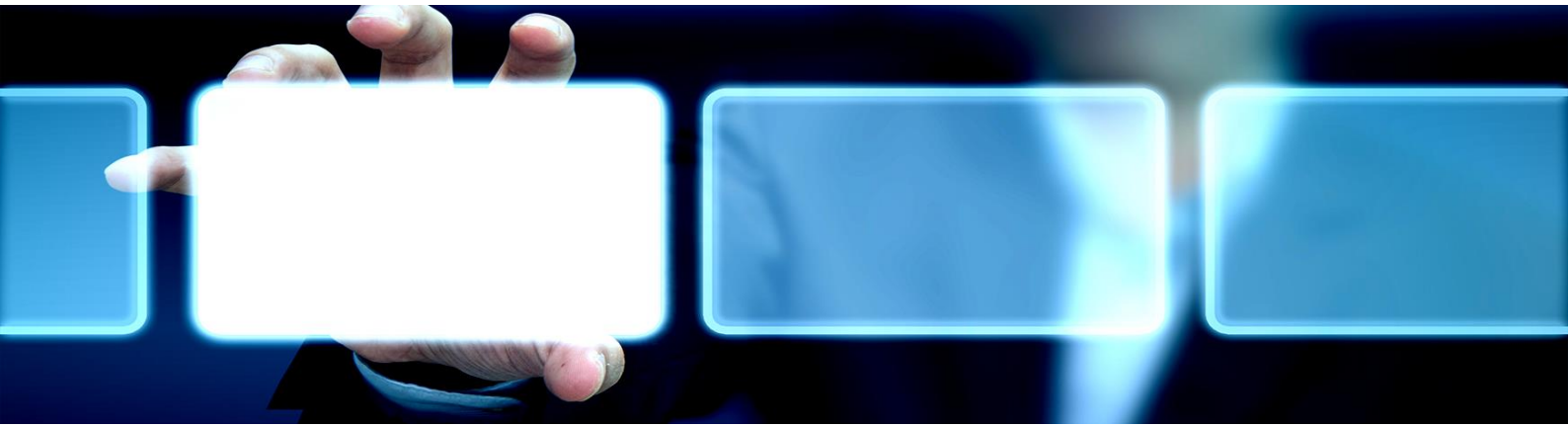
- customer experience;
- user access;
- service availability;
- internal and external network communications;
- device management;
- disaster recovery.

Successful IT-enabled operations enhance operational efficiency and reduce operational risk.

IDENTIFYING THE GAPS
IN INFORMATION TECHNOLOGY

This framework supports a more intentional view of small business IT. Aware that you need to pay equal attention to each of these four areas, you will be able to see where you're slipping. Falling behind on business technology can:

- hurt your competitive advantage;
- slow business processes;
- hinder innovation;
- frustrate customers;
- undercut employee engagement efforts;
- risk your compliance;
- lead to a damaging data breach or other downtime.



Your small business may be in a position to hire its own IT team, yet that puts the onus on you to find people to cover each of the framework areas. And it's a tight labor market, especially in IT. You'll need to recruit and train, and keep and develop the team, too. Or you could outsource your business tech to a managed service provider. More on that next.

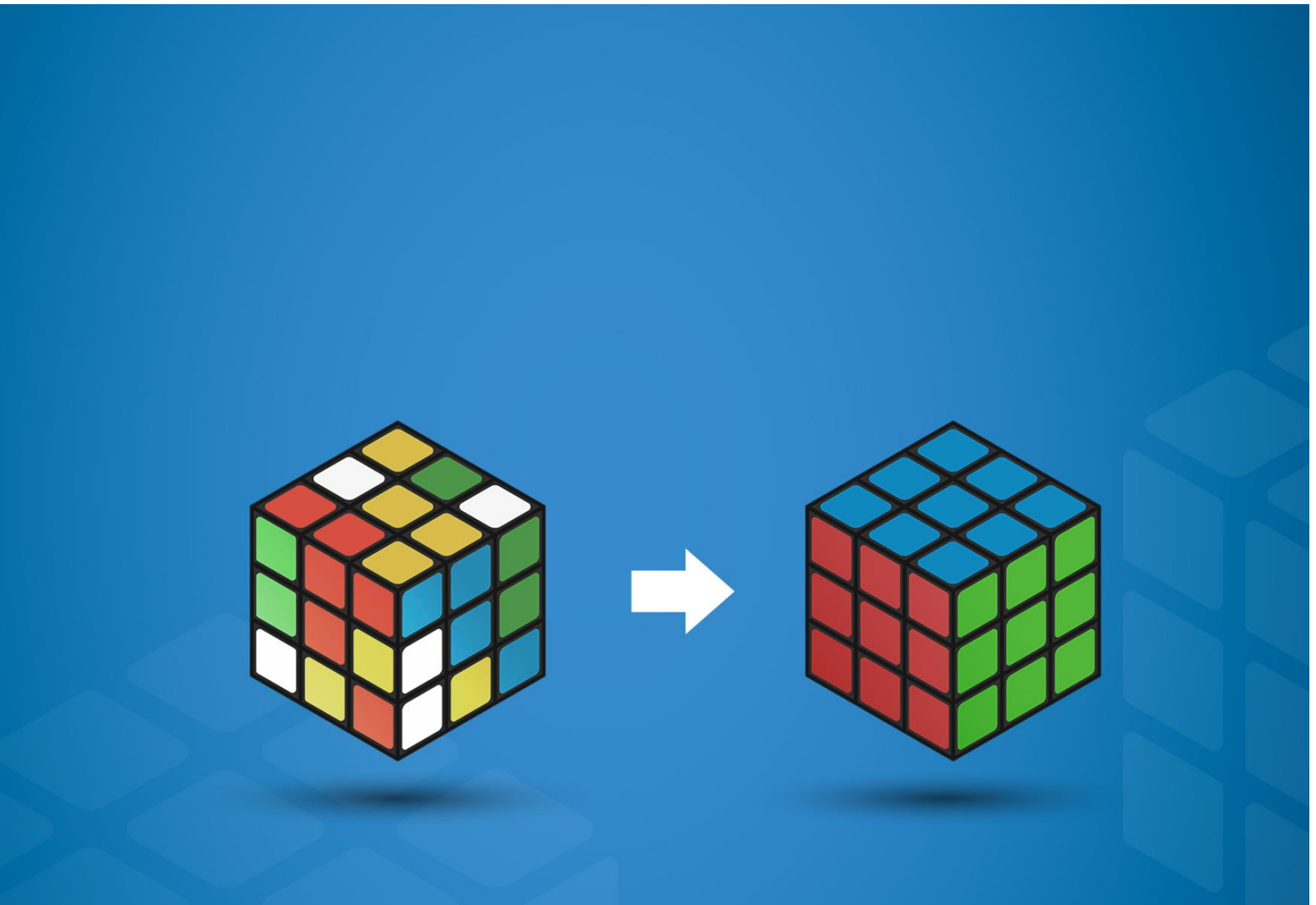
BENEFITS OF MSP PARTNERSHIP

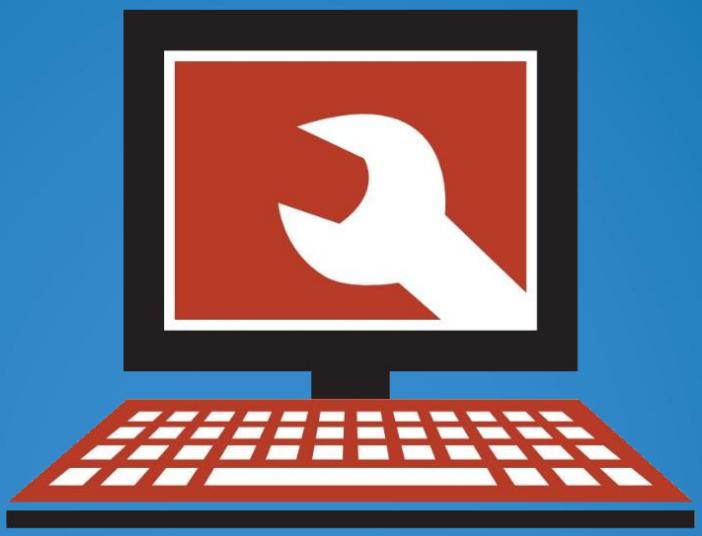
WE'RE HERE TO HELP

Working with an MSP, you gain access to IT experts with skills in all four framework areas. We keep current on tech stack innovation, security and compliance, and IT management and operations. It's not as daunting for us, because IT is our business.

An MSP gets to know your unique needs and suggests the best IT strategies. We can consult on the best hardware and software for your particular needs. We can manage your IT and secure your networks. We'll also spearhead digital business transformation for your business.

We're here to help. Contact us to learn more about our IT strategy and support offerings for small business.





hersTek.com

Phone: **570-779-4018**
Email: **support@herstek.com**
Web: **https://herstek.com/**
Facebook: **https://www.facebook.com/herstekllc**